E-Commerce Security: The Birth of Technology the Death of Common Sense?

Amidst the clamber to join the high-tech world of e-commerce, companies have neglected to apply common sense to their endeavours. It is arguably the lack of common sense rather than the lack of sophistication of e-commerce security which potentially will scupper e-trade development.

As Erma Bombeck once remarked, "[i]t seemed rather incongruous that in a society of supersophisticated communication, we often suffer from a shortage of listeners."[1] Butler has argued that "[a]lthough business was quick to recognise the advantages to be gained from improving connections to the outside world, a corresponding awareness of the unique vulnerabilities of such enhanced connectivity has been far slower to develop."[2] The lack of awareness can of course be attributed to the unavoidable fact that businesses' primary motivation is the creation of profit. Estimates[3] by The Gartner Group, for example, that e-tailing will grow to account for between 5-7% of total retail sales in North America by 2004 from the 1% figure it represented in 1999 serve only to fuel corporate profit drives. Analyst firm Forrester suggests[4] that worldwide Internet commerce will be worth $6,790 billion (*circa* £4,620billion) by 2004. The bulk of trade is likely to emerge from the USA, but, as Bennett notes, "…[the USA's] dominance will decline as European and Asian-Pacific countries expand their trading."[5] With the advent of m-commerce (*infra* at p.16), even that large rise will arguably pale into insignificance. Given such financial prospects, corporations may simply perceive that the delay caused by implementing e-commerce protection simply reduces their potential profit margin.

That corporations lack the requisite awareness is evidenced by the number of viral infections and the effectiveness of denial of service attacks their systems have been

subject to. As Millar has noted recently, denial of service attacks "…are the lead-lined cosh of hacking.."[6]. Numbering some 4,000 a week, such attacks have become, as Millar puts it, "..the weapon of choice for malicious hackers intent on inflicting most damage with the minimum of time and effort"[7]. The Internet provides the company with the means to contact and do business with the whole world. Butler maintains, however, that "…the downside to this ability is that other people are equally capable of reaching back into the company in the same way."[8] In January 1999, one individual stole information on more than 485,000 credit cards from an e-commerce site[9]. Some two weeks after that, data from 300,000 credit cards was stolen from the CD Universe web site[10]. In February 2000, a number of major e-commerce companies (including Amazon.com and Yahoo!) were subject to sustained denial of service attacks in which their web sites were so inundated with maliciously motivated requests for data that the sites' servers overloaded and could not deal with legitimate requests for information for a number of hours. The Love Bug[11] was described[12] as the most damaging and most widespread virus outbreak ever. Indeed, losses sustained in terms of lost work hours have been estimated to be in region of $10 billion. The Love Bug was opened as an innocuous looking e-mail attachment. The bug installed itself on the computers' hard drives, replaced itself with a copy of itself and sent infected e-mails to the addresses logged in the Outlook Express folder. The fact that Microsoft Windows runs on 9 out of 10 computers[13] made the bug particularly powerful and points, at an early juncture, the lack of corporations' common sense in placing their business eggs into one technological basket.

Ironically, Apple computers who have escaped the majority of destructive virus attacks because they do not operate using Windows software are now offering Microsoft compatible packages with their products. Market competition seems to

have overcome their common sense based logic and increased their future vulnerability to viral attack.

The security of e-mail is becoming an increasingly serious issue given that it is both a preferred mode of global communication and a common and simple vehicle for the introduction and dissemination of viruses and trojans. A virus has been likened, by Armstrong[14], to a burglar who breaks into a house, steals the contents and then leaves. A trojan (named after the famous Trojan horse of Greek mythology), on the other hand, is a burglar who breaks into a house repeatedly because he has established a way of gaining entry to the house without the homeowner ever becoming aware of the fact.

It is the convenience and user-friendly nature of e-mails which lies at the heart of the problem. As Butler notes, "[t]he rapid nature of e-mail exchanges seems to almost stun many users into a state of complacency in its use…"[15] It appears that many corporations' security warnings regarding, for example, the opening of attachments, go unheeded by employees and thus provide a vehicle by which viruses can infiltrate and disrupt corporations.

In October 2000, Microsoft was hacked using a QAZ Trojan horse. As with all Trojans, it entered the company's network as an ordinary e-mail attachment. Once the attachment was opened, the Trojan opened a 'back door' and allowed a blueprint for new software under development to be examined by the hacker. Norfolk maintains that "[t] he growing use of the Internet and almost universal use of certain software packages has greatly increased the threat from Trojans."[16]

The US National Infrastructure Protection Centre [sic] revealed[17] in December 2000 that it had traced several virus attacks likely to coincide with Christmas. Cluley of Sophos argues[18] that hackers exploit the feelings of Christmas spirit amongst

employees. He maintains that "[j]okes circulated by e-mail from system to system are exactly what people want, and virus writers specialise in attractive festive attachments such as screen savers, tunes and jokes."[19]

There is strong evidence that virus writers are getting more and more inventive and more and more technically proficient. Foresight [a group of experts from business, science, government and the voluntary sector which examines future trends] have argued that a "..clear danger.. is being at the mercy of a small technologically knowledgeable elite."[20] The increased skill-base of such hackers easily exploits the gullibility and lack of awareness of a number of e-mail users. A good example of this is the Naked Wife Trojan horse virus. It attached itself to an e-mail as 'NakedWife.exe' and the e-mail purported to come from a person that the recipient of the e-mail had just e-mailed. In the body of the message, the e-mail read "My wife never looked like that, best wishes (sender's name). It looked entirely genuine therefore. If opened however, the virus deleted critical system files whilst the recipient waited for the naked wife picture to load!!

Viruses such as the Love Bug, Anna Kournikova (similar to the Naked Wife virus except that it promised a photograph of the eponymous tennis star instead) and Naked Wife were totally preventable had companies ensured that an attachment procedure had been implemented and adhered to. The success of the viruses "..demonstrates that IT departments' non-adherence to common-sense security procedures is widespread."[21]

Cluley estimated that there are now some 4,000 new viruses each month, thirty of which go live on computer systems.[22]

Cluley notes an additional danger of lax e-mail protocol, which is that "..viruses contained in e-mails encrypted for security purposes will themselves be encrypted and

so will not be recognisable. This means the viruses that would otherwise be trapped will cross the company's firewall."[23] [A firewall (named after the barrier that stops a fire from spreading from a car engine into the passenger compartment) is the name given to hardware, software or procedures that provide access control to a company's computers]. Ironically, of course, businesses maintain that encryption is essential for their site and customer security.

Williams (of Axent Technologies) maintains that "[h]ackers do what they do for different reasons. Some do it for financial reasons. Some do it for financial reward, some for the intellectual challenge, some for the kudos within a certain society of hackers, others have political ends. It is up to the IT manager to determine which security threat group his or her company falls under and recommend installation of the appropriate security measures to combat the threat."[24]

Barrett suggests that this anti-hacker security programme may become easier in light of the fact that hacking itself has become easier. He suggests that "[t]he challenge, the fun, the game of hacking has passed, replaced by the thoughtless, aimless and amateur execution of tools written by others to exploit vulnerabilities."[25] Indeed, Foresight argue that "[a] general assumption about the future has been that the average individual will know more and more how to use technology but understand less and less how it works."[26]

Barrett argues therefore[27], that, if hacking is carried out by the less intellectually aware using widely available tools and techniques, a company need only learn to counter those tools and techniques and then incorporate those new-found solutions into their prospective security policy and procedures. Foresight have argued in this regard that "[i]nformation about how to compromise a system will be available more quickly and to more people. As the lingua franca of the internet, sites or

communication in English may disproportionately be targets for crime and disruption."[28]

More generally, it is argued that the problem of security owes much to the perception of security as an issue. Butler suggests that when debating security issues, "...people mistakenly persist in acting as though it is a problem that can be solved by the adoption of a solution."[29] Thus, Erwin argues, companies put their faith in nework intrusion products like firewalls. He suggests, however, that attempting to protect a company from every possible threat is "..a bit like trying to catch the Niagara Falls in a paper cup."[30]

Arguably, security is best addressed by adopting a position of inevitability, that is, "..understanding that things will go wrong, and that damage control measure must be in place to deal with failures when they occur."[31] From that position, the norm soon becomes one of creating a process of security. As Harold suggests, "[s]ecurity must be proactive to be effective and not simply based on reacting to the latest vulnerability."[32]

Ironically, given the importance of security in an environment in which security is perceived to be a very real threat, it is a function routinely delegated to already hard-pressed network or system administrators. As Netsec maintains, however, "[i]mplementing effective in-house network security…requires a number of distinct skills that are almost never found in a single person…"[33]

This lack of prioritisation and lack of expertise may then be exacerbated by naïve utilisation of those systems and procedures that may be in place. As Netsec suggests, "[b]uilding security-critical devices on top of proprietary, insecure operating systems will always create an opportunity for hackers."[34]

In some respects it is the required convenience of a corporation's operating systems that constitutes its self-created and promoted Achilles Heel.

Netsec confirm that on the whole, "..operating systems are designed to provide general functionality and ease of use."[35] Thus, "…networks are built first and security applied later."[36]

Yapp, of the Control Risk Group, maintains[37] that 80% of security breaches are caused by a company's own staff. As Goodwin argues, "[d]isgruntled former employees, people who are careless with their passwords, and dishonest staff with a little IT knowledge, can be far more devastating to a business than an external attack."[38] A survey[39] carried out this year by Pentasafe Security Technology has found that organisations typically spend 80% of their security budget protecting themselves against external threats, and only 20% on implementing internal security despite the fact that 80% of security breaches come from within companies. The Department of Trade and Industry in the UK reported this year that only 14% of UK companies had an information security policy.[40]

Even if a password is not written down, Yapp argues[41] that most can be established with a little deduction given that the apparent norm of password selection is to focus on names of family members, personal telephone numbers, favourite sports teams, etc. Erwin notes[42] that one of the most common passwords is, 'password'. The danger of over-reliance upon passwords as an essential part of a corporation's security measures may be seen most poignantly in Erwin's citation[43] of a merchant bank that this year laid off 5,000 staff without deactivating their passwords. Research revealed that 40% of the ex-employees had entered the network after their forced departure.

Another more infamous yet illustrative example of weak security infrastructure is the Barings Bank collapse in 1995. Although perceptually the bank was brought down by

one individual's reckless and unauthorised trading, in reality it was a range of ineffectual and uncontrolled systems which facilitated the rogue trading.

In July 1992, Leeson, the trader in question, instructed a computer clerk in Singapore to create an error account (number 88888, hereafter the 'error account'). He then instructed a systems engineer to amend the computer software so as to prevent the existence or contents of the error account from being divulged to London. The fact that Leeson was able to instigate these changes without fear of contradiction or adverse consequences, is the first point of concern.

Leeson's role for Barings Bank in Singapore had been to execute orders on behalf of colleagues based in Japan. Leeson then began to sell options without authority from Barings. An option provides the interested party with the right, but not the obligation, to buy or sell a set quantity (usually of currencies or securities) at some stage in the future in return for payment of a premium.

If the price rises in the interim, however, the loss can soon overshadow the original premium. This is what happened to Leeson but he simply hid the losses in the error account. Like a gambler is often wont to do, Leeson sold yet more options in a vain attempt to reduce his existing losses.

As far as Barings were concerned, Leeson was, judging by the amount of premiums he provided them with, a raging success. In reality, he was bringing them closer and closer to collapse. By December 1994 he had accumulated losses on the error account of some £208 million, and by February 1995, the accumulated losses on the error account amounted to £830 million[44]. Drummond argues that "[s]ecurity frequently involves designing systems of control to prevent unauthorised access. Baring's collapse suggests that organisations may have more to fear from authorised users apparently going about their daily business."[45]

The key problem for Barings lay in both its weak operational control and its weak application of its computer systems and processes.

Leeson controlled the trading office and the office in which documentation relating to his trading was processed. This lack of effective segregation allowed Leeson to disguise his losses.

As Drummond argues, "[p]rotecting systems from insider abuse is difficult because organisations require control and flexibility."[46]

Leeson exploited Barings' lack of control and not only created the error account but ensured that its contents never came to the attention of London. Drummond notes that "[r]isk assessment typically concentrates on control points with greatest vulnerability and potential loss."[47]

Leeson's ability to achieve his deception lay in the simple fact that Barings never anticipated his actions. Ironically, in 1992, Leeson had been assigned to a team in Tokyo charged with investigating allegations of internal fraud. As Drummond confirms, "…the least consequential parts of the system are potentially highly vulnerable to abuse precisely because they are unguarded."[48]

It was ironic, therefore, that despite his best endeavours, details of Leeson's error account **did** in fact reach London. In other words, the Barings Bank software **had** worked. The lack of control of the system, however, enabled Leeson's actions to continue to go unnoticed. The system in London could not correlate the contracts in the error account with existing account numbers and so, rather than raising a query, simply placed them in a suspense file. The suspense file was only noticed after Barings had collapsed. The suspense file should have been routinely and regularly audited. It was not.

"Curiousity killed the cat". Lack of curiousity killed Barings.

As Drummond puts it, "[f]raud invariably generates evidence of its existence."[49] Barings' systems allowed evidence to be disguised and hidden and, even when in the open, ignored the evidence because it did not correlate with existing account details. The lack of correlation, if nothing else, should have generated a concerned and active response from Barings. As Drummond notes, "[t]o neglect such clues is to behave like the drunk who looks for his car keys not where he left them, but under the lamp post because the light is good."[50]

The same ignorance of security protocol and the implicit trust placed in employees evidenced in the Barings fiasco can also be detected in the recent case involving FBI spy, Robert Hanssen. Hanssen helped to set up the FBI's Intelligence Investigative System into which agents placed the names, addresses etc of their Soviet targets. This gave Hanssen access to the true names of every FBI intelligence source in New York. He also worked with the intelligence specialists who installed bugs and cameras to watch over Soviet officials. Thus, he knew where every watching and listening device was placed. Aside from that, he was generally very inquisitive about every activity going on around him. A former colleague simply remarked that "I just figured he was nosy."[51]When he was posted to Washington Hanssen was given increasingly important assignments which, according to McGeary, allowed him to "..poke unnoticed into virtually every corner of government intelligence, surveying a complete library of sources, methods, techniques, targets, plus secret-operations plans and analytical assessments."[52] The FBI trusted Robert Hanssen and therefore mistook his insatiable interest in the Agency's activities for keenness rather than espionage. Effective security (in terms of both systems and processes) will never come cheap, and inevitably, therefore, financial commitment may also become an issue for corporations. Netsec cogently argues that "[b]udgets for network security are usually

owned and managed by the people who are responsible for functionality. In times of limited budgets, functionality always wins at the cost of security."[53]

Xephon indicates that corporations have a disturbingly lax attitude to security. Their report[54] examined the attitudes of IT managers worldwide regarding security issues and e-business success. One third of respondents said that security concerns slowed down progress of their firms' e-business development. One in six IT managers felt that e-business was awarded greater importance than security matters.

An exacerbation of the afore-mentioned factors may lie in the tendency of corporations to succumb to the pressures of joining the world of e-commerce at the expense of creating an adequately tested security system.

The Gartner Group reported[55] that half of all small and medium sized businesses would fall victim to internet attacks by 2003. Smaller firms are driven to e-commerce conformity but lack the technical or financial wherewithal to do so safely.

The Gartner Group argues that smaller companies tend to rely upon part-time staff, or staff without appropriate qualifications to run enterprise servers. In addition, they depend upon their Internet Service Providers (ISPs) to provide their security. This could open up their partners to intrusion. If, as seems likely, small firms are hacked or subject to viruses, they could, as Cyrano predicts[56], become a weak link in the arguably already tenuous e-market, rendering larger firms vulnerable to attack.

Mannion argues that "[s]ecurity is only as strong as its weakest link. It should be kept in mind where business to business links are created."[57] Ironically, even if a large corporation has an effective security system in place, such corporations "…are now linked to suppliers and customers who do not see security as a main business objective. A hack attack could be launched through one of these sites."[58]

Security, as Barings discovered to its cost, should be contained within a process of overarching security not merely or primarily within a package containing an anti-viral device. Mitnick suggests that to assume that the installation of a firewall will protect the company form a full range of security threats is naïve in the extreme. Specifically, "[t]hat assumption creates a false sense of security, and having a false sense of security is worse than having no security at all."[59]

PowerGen, a UK electricity supplier, made a number of elementary errors in the process of security which served to undermine any security systems they had in operation. They held files of customer records on their Web server rather than on a separate server. They failed to encrypt the data contained on those files. As a consequence, bank details of 2,500 customers were accessible via their standard website.

The Association of British Insurers predicts[60] that cyber crime will increase substantially in the next twenty years. They maintain that access to information is very much a double-edged sword since "[w]e are increasingly reliant on the smooth flow of information. Any disruption is, at best inconvenient, and, at worst, life threatening."[61]

The perceived inconvenience of obeying a system of security as it relates to communication has led to convenience above security becoming the driving force. Consequently, public key infrastructure (PKI) systems with digital certificates and digital signatures have promised to protect the sanctity of online communications. [Public Key Cryptograpy utilises pairs of huge numbers used to encode and decode messages. One number (the public key) is published. The second number is a private key kept secret. One key is used to encode the message, the second key to decode it.] Uptake of PKI systems is on the increase.

It has been argued, however, that "…digital signatures bind documents to computers, not to people - and this can be a security weakness."[62] Foresight have argued that "[e]lectronic signatures offer two potential routes for those seeking to commit a crime; either personification of a person/signee…or the forgery of the actual signature…"[63]

In ordinary, land-based transactions, it is argued that hand-written signatures are not automatically acceptable for important transactions and that notarised signatures are used instead. In addition, of course, it is an accepted principle of ordinary consumer dealing that the credit card holder's signature is witnessed by the person they are purchasing goods from.

The US National Notary Association argues that the same caution should be exercised in relation to digital signatures. They suggest that "[a]s industry becomes more digital, it becomes possible to reproduce and take on the identity of another (person)."[64] Summers notes that "[t]he Internet permits a risk-free anonymity that has emboldened a new generation of forgers and identity thieves."[65] According to Summers[66], complaints of identity theft rose from less than 40,000 in 1992 to 750,000 in 1999. The importance of basic corporate systems security becomes self-evident when the propensity for breaching those systems is revealed and recognised.

Most web-based companies routinely employ 'cookies'. These are small (4K) pieces of information sent from the web server to the browser and then stored on the user's hard disk. When that user re-visits the site in question, the cookie is automatically returned to the server. The cookie allows the user to be recognised as a former visitor to the site. It facilitates a cyber form of the greeting a loyal customer might receive in a land-based store. In theory, being greeted by name on a website encourages repeat client patronage.

If a bug is introduced, however, the cookie can become the cookie monster, a potential threat to the consumer.

In May 2000, for example, a flaw in Microsoft's Internet Explorer emerged which allowed any server to read cookies belonging to other sites. This, known as the 'Open Cookie Jar'[67], allowed hackers to monitor browsing habits.

Microsoft then admitted, in October 2000, that there was a security weakness which allowed hackers to read and execute files on web sites powered by its Internet Information Services (IIS) software by simply requesting a specific web address.

The afore-mentioned difficulties over security breaches may be categorised as what Schneier refers to as 'syntactic'[68] attacks, namely active exploitation of software and hardware vulnerabilities, gaining unauthorised access to sites and organising denial of service attacks.

He argues that the next wave of attacks will be 'semantic'[69] in nature - exploiting what he terms "human-computer interaction."[70] His illustrative example concerns the firm of Emulex. Mark Jakob posted a false press release to a service called Internet Wire. The release falsely maintained that Emulex's Chief Executive was stepping down and that the company needed to restate its earnings. Within hours, the company's stock price fell from $70 to $40 per share. Luckily, the share price did recover once the hoax had been discovered but the cost to investors was $110 million.[71]

In April 1999, visitors to an online financial news message board operated by Yahoo got a scoop on PairGain, a telecommunications company based in California. An e-mail posted on the message board under the title "Buyout News" said that the company was being taken over by an Israeli company. The e-mail also provided a link to the website of the Bloomberg News Service which contained a detailed news story

of the takeover. As news of the takeover spread the company's publicly traded stock shot up by more than 30% and the trading volume to seven times its usual rate. The entire story was false and the website was not Bloomberg's but a counterfeit copy. When news of the hoax spread, the price of the stock dropped sharply and caused massive losses to investors who had bought stock at artificially inflated prices.[72] The Office of Internet Enforcement set up by the Securities and Exchange Commission has reported similar cases of bogus company takeover scams (also known as 'scalping', 'pumping' and 'dumping' or 'ramping'.

The security issues described thus far relate only to fixed computer systems, controllable, however ineptly, *in situ.*

The flaws identified in processes and systems will arguably pale into insignificance if m-commerce begins to take effective shape. M-commerce[73] refers to the buying and selling of goods and services through wireless handheld devices such as cellular telephone and personal digital assistants (PDAs). M-commerce effectively provides for access to the Internet without the necessity of plugging directly into a computer terminal. The key technology for m-commerce is Wireless Application Technology (WAP). M-commerce will potentially affect a wide range of industries[74] including financial services (including mobile banking, when customers use handheld devices to access their accounts and pay bills, and brokerage services where customers can see stock quotes and trade), telecommunications, in which bill payment can be conducted on the handheld device, and service/retail, where customers can place orders and pay for those orders from their handheld devices.

It has been predicted that m-commerce will be launched firmly once third generation (3G) cellular services become routinely available. 3G services will provide a permanent internet connection and data throughput will be higher, matching at least

today's 56kbps modems. International Data Corporation argue[75] that the number of wireless devices with two-way access to the Internet is expected to increase to 61.5 million by 2003.

It is suggested that companies will be able to offer services and products to consumers via mobile handsets in much the same way as they can over the web today.

The Gartner Group predicts that the number of mobile connections to the internet will top one billion world-wide by 2003. It further predicts that the consequential global value of transactions by mobile device will rise to $1.8 trillion by 2005[76] (assuming an ideal business environment). As Armstrong notes, "[b]usinesses, enthusiastically examining mobile commerce…are incessantly looking for ways to widen their reach and fatten revenues."[77]

In order to be as successful as these predictions, however, the mobile phones and PDAs (Personal Digital Assistants) will have to be extremely rapid and efficient in data transfer and retrieval. The problem with wireless technology, according to Chen[78], is of course that they have a limited memory. In terms of marketability, as with ordinary landbased computer systems, manufacturers will dedicate memory to efficient utility rather than efficient, but memory depleting, encryption and authentication systems. If cell phones and PDAs are stolen (which, given the general propensity for thieves to take ordinary office based computers, will be exacerbated by the smaller size of m-devices) then the absence of effective security measures might be devestating for the individual and his/her corporation if those devices fall into even partly competent hands.

Medina's survey[79] of 3,000 people found that almost no handheld owners used anti-virus protection even though 81% of the sample stated that they were worried about future viruses that could infect their mobile devices.

It is suggested that the threats to m-commerce will increase in proportion to the speed and higher bandwidths of the mobile devices. They will of necessity be able, for example, to receive and re-distribute e-mail attachments. These are of course perfect vehicles for Trojan horses back into the company. In June 2000, experts intercepted Timofonica (a virus similar to the Love Bug) designed to attack cell phones with text capability and in September 2000, experts warned of the Liberty Crack virus, a PalmPilot Trojan horse that deleted files.

Anti-virus company, Trend Micro, argues that as "…mobile devices with always-on connectivity become widespread, we will see more and more viruses targeted at [mobile] platforms."[80]

In terms of technological ability currently available, Robinson notes[81] that phones which can be used in all countries pose a potential threat. Researchers have found a design problem in GSM phones. The GSM (Global System for Mobile Communications) is the most popular mobile phone system in the world, with 65% of the total digital market. GSM includes a facility to encrypt data travelling across the network. Western Europe, however, cannot export encryption products to certain countries (for example, those against whom there are UN sanctions) and so the default version of the GSM protocol does not use encryption.

It is possible to build an unauthorised 'base station' (the hardware which communicates with the handset) that jams the signal from the real station and forces the mobile phone to connect with it. The false base station tricks the encryption ready non-European handset into believing that the message is being sent from a foreign country, e.g. Iraq, in which encryption may not be used. Consequently, the message remains unencrypted and the open message is received by the false station. This so-called 'Man in the Middle (MITMA) attack allows the false station to intercept

messages between the real station and the handset without either being able to detect it. Even with this scenario, those who will profit from the upsurge in m-commerce insist that it is not a security issue. James Moran, fraud and security director at the GSM Association argued that building such an interception device would require considerable technical skill[82]. Furthermore, he noted that "[w]e know about it as a technical issue, but we haven't seen it demonstrated."[83] In other words, we'll just wait and see. By that time of course it will be too late. As this view is expressed by a company with a vested interest in establishing that there is little current threat to GSM phones it is understandable even if still not acceptable. More worrying, perhaps, is the fact that some anti-virus firms have suggested that the fears expressed by Trend Micro (*supra*, at p.18) are premature. As Sophos, for example, noted, "[v]iruses for mobile devices are easy to create but they don't spread well. There may be a need for protection on wireless products in the future, but not yet."[84] Similarly, Kroll (director of security for Finjan Software) argued (in March this year) that the threat of mobile-specific viruses was several years away. As he put it, "[v]irus writers gravitate to what is easiest and effective. Why do something through a PalmPilot when you can go directly to a PC?"[85] Such ineffectual, unimaginative and non-lateral short-term thinking, which would have consigned the Wright brothers to rapid obscurity, will inevitably result in long-term terminal failure.

A survey conducted by BindView[86] noted that only 12% of a thousand companies surveyed had a policy regarding communications over mobile networks. Twenty-seven percent said employees used notebook PCs at client premises and 37% said staff worked from home via remote access to the corporate network. This, according to BindView, "..opens up communications to hackers who could access cached user names and passwords."[87] Finally, 53% of managers said their IT department often had

no idea where company laptops were and that when in employees' homes, most were lent to friends or flatmates[88]. It is somewhat ironic perhaps, that the QAZ trojan attack upon Microsoft (mentioned *supra* at p.3) is alleged[89] to have been perpetrated via a Microsoft employee's home computer connected to the network.

A survey in 2000[90] of risk managers in large corporations in the US and Europe revealed that "[b]usinesses do not adequately understand the risks posed by technology, have difficulty identifying potential risks and lack the tools to manage them effectively.."[91]

More precisely, although computer/internet risk was the number one concern of European companies and the number two concern of US companies, only 30% of the former and 25% of the latter had formal management structures in place to manage technology risk. Only 60% of US companies and 56% of European companies had implemented employee training programmes as part of their programmes to manage security risk. Furthermore, about 75% of US executives and 60% of European executives said their employees had only a "fair" or "poor" understanding of technology risks.

Finally, the issues of security now need to be placed within the context of globalisation. As Lovaas has noted, "[t]he global nature of e-commerce, varying legal systems and the speed with which new innovations are brought to market further complicate the challenges facing companies today, leading many firms into uncharted waters of liability risks as well as those which affect their revenue streams."[92]

Foresight, similarly, have noted that "[a]s the global reliance upon interconnected computer systems increases, so will the need to instigate protective measures against failure and malicious attacks."[93]

There is a constant, even if laudable, pressure from organisations such as the OECD (Organisation for Economic Co-operation and Development) for e-commerce development. In their recent (January 2001) Progress Report on the OECD's Work on Electronic Commerce they argued that "[e]lectronic commerce is a central element in the OECD's vision of the tremendous potential that our networked world now holds…"[94]

Ironically, they posit that "[t]rust is central to any commercial transaction. Developing new kinds of commercial activities in the electronic environment largely hinges on assuring consumers and businesses that their use of network services is secure, reliable and verifiable."[95]

On the other hand, the OECD in its Issues Paper[96] tantalises prospective e-businesses with salient likely values of e-commerce of $US 650 billion worldwide with some projections of up to a ten-fold growth over the next few years.

However, the OECD then maintain that "[v]isions for the rapid growth of electronic commerce are predicated on successful resolution of concerns about the lack of adequate infrastructures, skills and capabilities and the security of transacting business or interacting with service providers in electronic environments."[97]

Besides the lack of such commitment in developed countries, the OECD points out that in the areas of the world for whom globalisation is a key to development, "[t]here are differences in business practices, legislative frameworks, infrastructure deployment and the general social and economic conditions within countries."[98]

The Economist Intelligence Unit and Pyramid Research have recently introduced a concept of 'e-readiness', which they define as "… the extent to which a country or market's business environment is conducive to Internet-based commercial opportunities"[99]. In an appraisal of the world's sixty largest economies, Singapore

was ranked seventh and Hong Kong thirteenth. China, however, was placed at forty-fifth position. To contextualise this, India was placed at forty-ninth. The key reason for China's relatively low position was attributed to the fact that "..poverty, illiteracy and infrastructure inadequacies prevent e-business from gaining critical mass.."[100] Ironically, of course, China is reputed to have an internet population of 5.2 million which is expected to double to 10.4 million by the end of this year[101]. As Thompson notes, however, "[e]-commerce is still in its infancy due to poor quality of service, security and the absence of a convenient payment method."[102] President Jiang Zemin has nevertheless maintained that "[w]e should recognise the tremendous power of IT and vigorously promote its development."[103] The potential danger for China lies precisely in the fact that the conduit running between significant financial gain and wider internet accessibility is blocked. According to a Chinese government spokesperson[104], China's credit system is deemed to be chaotic and prone to fraud and other crimes. It does not have an electronic currency payment system, it does not have a modern goods delivery system and its national information grid is not sufficiently large to facilitate the connection of all of its retailers.

If China's internet economy continues to attempt to respond, without the requisite security, regulation and infrastructure *in situ*, to the global pressure to engage in e-commerce, then the scope for e-commerce abuse will be vast. Reuters has commented[105] upon China's requirement for all web sites that provide or release information on the World Wide Web to undergo security checks and approval. As Reuters notes, "[a]uthorities are anxious not to smother the Internet, keenly aware that new information technology is key to China's economic future. Yet they fear an information free-flow which could threaten communist control."[106] Within the context of e-commerce development these two concerns remain diametrically opposed. The

very nature of the internet and its on-going development and success rests precisely upon its actual or perceived extraterritoriality. As Zekos has suggested, "…cyberspace cannot be combined in any single territory and assuming that territoriality is the single basis for jurisdiction then no state could regulate cyberspace."[107] Attempts to control the sites in this way can only lead to eager business communities both within and without Chinese borders disguising their internet sites as something less politically overt or, in the case of non-China based sites, carrying on regardless. If legitimate businesses do this, illegitimate entities (whether hackers or organised crime groups) will capitalise upon such subterfuge simply by attaching themselves to the sites of those legitimate but non-sanctioned businesses. Savona, et.al. argue that criminal organisations "…go where opportunities are and the process of globalisation helps their expansion."[108] Indeed, "[a] wider market in a world afflicted by strong economic inequalities means a larger number of occasions for crime against business."[109]

If China maintains a belief that its outlawing of certain sites is effective then such infiltration will go unhindered and uncontrolled. It is noteworthy, perhaps, that the security breaches discussed elsewhere in this paper have occurred in those industrialised nations deemed to be at the very apex of technology.

Ironically, the UK government, whose thought process will be replicated by many governments, notes the dangers inherent in e-commerce and m-commerce. A document produced by the National Infrastructure Security Co-Ordination Centre notes that "IT systems in government, business and elsewhere are becoming increasingly interconnected, creating national and global IT networks. This opens up unprecedented benefits for businesses but at the same time creates new vulnerabilities in our IT systems, which could be exploited by the ill-intentioned."[110] The Centre argues that "[g]overnment has a responsibility to ensure that protection, proportionate

to the threat, is in place for systems critical to national well-being and economic prosperity."[111]

How ironic, therefore, that the myriad of businesses and the vast range of computer systems and devices they employ are unable or unwilling to cope with the array of attacks and intrusions they currently face. They have been driven by the pressure and desire to board the e-commerce and m-commerce trains. They have routinely underestimated the threats of e-commerce even when such threats were, and continue to be, readily identifiable. They seem likely to ignore m-commerce threats altogether because common sense tells them that the threat is as yet undeveloped. That will be their ultimate downfall and mark the beginning of the end for a successful global economy. If China fails to learn, from the previous and on-going experiences of other more established economies, of the necessity of placing common sense above economic desire, it will lose not only its share of the global e-market but more crucially, leave itself open to a sustained and debilitating attack from the criminal fraternity from which it will find it extremely difficult to recover.

---

[1] *'Bits & Pieces'*, March 22, 2001, p.3.
[2] Butler, M, *'Managing Risk'*, E-Business Review, October 2000, Volume 1, Issue 7, p.59.
[3] Provided in E-Commerce Times, June 28, June 19, 2000, www.ecommercetimes.com.
[4] Cited in Bennett, M, *'Online Firms Must Go Global'*, IT Week, 22 January, 2001, p. 25.
[5] *ibid*.
[6] Millar, S, *'Teenage Clicks'*, The Guardian, G2, June 5, 2001, pp.2-3, at p.2.
[7] *ibid*.
[8] Butler, M, *op.cit.*
[9] Reported at www.zdnet.co.uk/news, March 17, 2000.
[10] *ibid.*
[11] A generic name for a virus which was disguised as an e-mail message proclaiming "I LOVE YOU" to its unlucky recipients.
[12] Hodges, G, President and CEO of McAfee, in Grossman, L, *'Attack of the Love Bug'*, Time, May 15, 2000, pp. 25-30, at p.28.
[13] *ibid.*
[14] Armstrong, I, *'Defending Today's Troy'*, www.westcoast.co./securecomputing/2000_05/second/feature.
[15] Butler, M, *op.cit.*
[16] Norfolk, D, *'Trojan Code Opens Up Back Door for Hackers to Access Systems'*, IT Week, 27 November, 2000, p.55.
[17] Cited in Lee, C, *'Viruses and Hacking for Xmas'*, IT Week, 11 December, 2000, p. 5.
[18] *ibid.*
[19] *ibid*.

[20] *'Just Around the Corner'*, www.foresight.gov.uk, para.2.13 at p.6.
[21] Cluley, G, in Williams, P, *'Firms Ignore Virus Patch'*, IT Week, 15 January, 2001, p.10.
[22] *ibid*.
[23] *ibid.*
[24] Cited in Lee, C, *'Top Managers Ensure Security'*, IT Week, 18 December, 2000, p.42.
[25] Barrett, N, *'Hackers Lose the Game'*, IT Week, 18 September, 2000, p.19.
[26] 'Just Around the Corner', *op.cit.*
[27] Barrett, N, *op.cit.*
[28] *'Just Around the Corner'*, *op.cit*, para.2.5 at p.4.
[29] Butler, M, *op.cit.*
[30] Cited in Street, M, *'Making Security a User Issue',* IT Week, 26 March, 2001, p.51.
[31] Butler, M, *op.cit*.
[32] Cited in Kavanagh, J, *'Security is a Staff Issue'*, Computer Weekly, 20 July 2000, p. 48.
[33] *ibid.*
[34] *ibid*.
[35] *ibid.*
[36] *ibid.*
[37] Cited in Goodwin, B, *'Cybercrime – An Inside Job'*, Computer Weekly, 31 August, 2000, p.16.
[38] *ibid.*
[39] Reported in IT Week, 19 February, 2001, p.36.
[40] Reported in IT Week, 26 March 2001, p. 51.
[41] Cited in Goodwin, B, *op.cit.*
[42] Cited in Street, M, *op.cit.*
[43] *ibid.*
[44] www.newsrisk.ifci.ch/135260.
[45] Drummond, H, '*The Maginot Line Syndrome'*, Computer Weekly, 21 September, 2000, p.54.
[46] *ibid*.
[47] *ibid*.
[48] *ibid*.
[49] *ibid.*
[50] *ibid*.
[51] McGeary, J, *'The FBI Spy'*, Time, March 5, 2001, p.39.
[52] *ibid.*
[53] Cited in Kavanagh, J, *op.cit.*
[54] Cited in Bennett, M, *'Strategies for Fighting Fraud'* IT Week, 22 January, 2001, p.39.
[55] Reported in Neal, D, *'Small Firms Raise Insecurity'*, IT Week, 23 October, 2000, p.16.
[56] *ibid.*
[57] Cited in Doyle, E, *'Half of SMEs on Net Will be Hacked in Three Years'*, Computer Weekly, 26 October, 2000, p.4.
[58] *ibid.*
[59] Cited in Chen, A, *'Poacher Advises Gamekeepers'*, IT Week, 9 October, 2000, p.45.
[60] *Future Crime Trends in the United Kingdom*, cited in Neal, D, *'Net Crime Set to Rocket'*, IT Week, 4 September, 2000, p.15.
[61] *ibid.*
[62] Townsend, K, *'Experts Warn of PKI Dangers'*, IT Week, 11 December, 2000, p.48.
[63] *'Just Around the Corner', op.cit*. 3.10 at p. 13.
[64] Townsend, K, *op.cit.*
[65] Cited in Townsend, *op.cit.*
[66] *ibid*.
[67] Townsend, K, *'Why Cookies Cause Upsets'*, IT Week, 28 August, 2000, p. 36.
[68] Defined in Sullivan, E, *'Garbage In, Trouble Out'*, IT Week, 6 November, 2000, p.26.
[69] *ibid*.
[70] *ibid.*
[71] Lemos, R, *'Security a Low Priority in Y2K'*, www.zdnet.co.uk/news/2000.
[72] Reported *in 'The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet'* (A Report of the President's Working Group on Unlawful Conduct on the Internet), March 2000, www.cybercrime.gov/unlawful.
[73] As defined at www.whatis.techtarget.com.
[74] *ibid.*

[75] Reported in Chen, A, *'M-commerce Security a Moving Target'*, www.zdnet.com/eweek
[76] Reported in IT Week, 18 September, 2000, p.70.
[77] Armstrong, I, *'Fighting for Mobile Security'*, www.westcoast.com/securecomputing/2001_02/special.
[78] Chen, A*, 'M-commerce Security a Moving Target', op.cit*.
[79] Reported in Lemos, R, 'Handhelds: Here Come the Bugs?', www.zdnet.com/zdnn/stories/news.
[80] Reported in IT Week, 26 February, 2001, p.4.
[81] Robinson, S, *'Design Flaw in Mobile Phone Protocol Opens Security Hole'*, IT Week, 25 September, 2000, p.52.
[82] Reported in Robinson, *op.cit.*
[83] *ibid.*
[84] IT Week, 26 February, 2001, p.4.
[85] Cited in Lemos, R, *op.cit.*
[86] Reported in Neal, D, *'Firms Fail to Tackle Mobile Security Risk'*, IT Week, 23 October, 2000, p.6.
[87] *ibid.*
[88] *ibid.*
[89] www.zdnet.co.uk/news/2000.
[90] *'The E-Frontier: New Challenges to Corporate Risk Management'*, www.stpaul.com/cyberrisk-survey.
[91] *ibid.*
[92] i*bid.*
[93] *'Just Around the Corner', op.cit*. 2.9 at p. 5.
[94] *'Progress Report on the OECD's Work on Electronic Commerce'*, 16-17 January, 2001, www.oecd.org, p. 3.
[95] *ibid*, p. 6.
[96] *'Issues Paper: OECD Emerging Market Economy Forum on Electronic Commerce'*, www.oecd.org, p.4.
[97] *ibid*.
[98] *ibid*.
[99] Reported in Perez, B, *'Hong Kong Seen as "E-ready", Willing and Able'*, South China Morning Post, May 9, 2001, www.technology.scmp.com.
[100] *ibid*.
[101] Thompson, V, *'Surfing the Dragon'*, Computer Weekly, 7 June, 2001, p. 71.
[102] *ibid*.
[103] Reported in Thompson, V, *op.cit*.
[104] Chen Wenling, Assistant Director of the Industry, Transport, Trade and Economic Devlopment Department, speaking on 25 January, 2001 at www.chinaonline.com/issues/internet_policy.
[105] 'China Hits Internet With Secrecy Rules', cited at www.zdnet.co.uk.
[106] *ibid.*
[107] Zekos, G, *'Internet or Electronic Technology: A Threat to State Sovereignty'*, The Journal of Information, Law and Technology, Issue 3, 1999, www.elj.warwick.ac.uk/jilt/99-3/zekos.
[108] Savona, E, et.al. *'Globalisation of Crime: The Organisational Variable'*, www.jus.unitn.it/transcrime/papers, at p.2.
[109] *ibid*, at p.4.
[110] Reported at www.niscc.gov.uk.
[111] *ibid.*